KAPLAN FOX & KILSHEIMER LLP
Laurence D. King (SBN 206423)
Matthew B. George (SBN 239322)
Blair E. Reed (SBN 316791)
Clarissa R. Olivares (SBN 343455)
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Telephone: 415-772-4700
Facsimile: 415-772-4707
Email: *lking@kaplanfox.com*
mgeorge@kaplanfox.com
breed@kaplanfox.com
colivares@kaplanfox.com

BONI, ZACK & SNYDER LLC
Michael J. Boni
Joshua D. Snyder (*pro hac vice application forthcoming*)
Benjamin J. Eichel (*pro hac vice application forthcoming*)
15 St. Asaphs Road
Bala Cynwyd, PA 19004
Telephone: (610) 822-0200
Facsimile: (610) 822-0206
Email: *mboni@bonizack.com*
jsnyder@bonizack.com
beichel@bonizack.com

Attorneys for Plaintiff and the Putative Class

[Additional Counsel on Signature Page]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JULIE MACMILLAN, individually, and on behalf of all others similarly situated,

Plaintiff,

v.

23ANDME, INC.

Defendant.

No. 3:24-cv-0555

CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiff Julie MacMillan ("Plaintiff"), individually and on behalf of herself and all others similarly situated, alleges the following against 23andMe, Inc. ("23andMe," the "Company," or "Defendant"). The following allegations are based upon Plaintiff's personal knowledge with respect to herself and her own acts and, following her investigations and the investigation of her counsel, upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against 23andMe for its failure to properly secure and safeguard Plaintiff's and similarly situated individuals' personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information"), including but not limited to their name, sex, date of birth, genetic information (including but not limited to "Maternal and Paternal Haplogroup results" and "Neanderthal Ancestry results"), predicted relationships with genetic matches, ancestry reports, ancestors' birth locations and family names, family tree information, profile pictures, and geographic location.[1]

2. 23andMe purports to be a leading consumer genetics and research company, founded in 2006, that describes its mission as helping people access, understand, and benefit from the human genome. According to the "Corporate Profile" on its website, 23andMe touts itself as having "pioneered direct access to genetic information" as "the only company with multiple FDA clearances for genetic health reports.[2]

3. As of March 31, 2023, 23andMe cumulatively possessed and stored the Private Information of over 14.1 million people in its databases.[3] This Private Information includes genetic information provided by individuals since 2006 in connection with the Company's "Personal

[1] 23andMe Blog, Addressing Data Security Concerns, 23andMe, Inc., https://blog.23andme.com/articles/addressing-data-security-concerns (last accessed Dec. 7, 2023); Lily Hay Newman, *23andMe User Data Stolen in Targeted Attack on Ashkenazi Jews*, Wired (Oct. 6, 2023), https://www.wired.com/story/23andme-credential-stuffing-data-stolen/ (last accessed Dec. 7, 2023).

[2] 23andMe Investor Relations, *Corporate Profile*, 23andMe, Inc., https://investors.23andme.com/ (last accessed Dec. 7, 2023); *see also* 23andMe Annual Report (Form 10-K) FY Mar. 31, 2023 (May 25, 2023) ("FY 2022 10-K") at 65.

[3] FY 2022 10-K at 69.

Genome Service" business, which purports to provide consumers "with a broad suite of genetic reports, including information on customers' genetic ancestral origins, personal genetic health risks, and chances of passing on certain rare carrier conditions to their children, as well as reports on how genetics can impact responses to medication."[4]

4. This class action is brought on behalf of all citizens in the United States who are the victims of a targeted cyberattack on 23andMe that occurred on or around August 11, 2023 or prior thereto ("the Data Breach").

5. According to news reports, "[o]n August 11, a hacker on a known cybercrime forum called Hydra advertised a set of 23andMe user data."[5] The hacker claimed "to have 300 terabytes of stolen 23andMe user data" that they would sell for $50 million and offered to sell "a subset of data" for between $1,000 and $10,000.[6] The hacker also purportedly indicated that they had contacted 23andMe, but the Company's response was ineffectual.[7] At least one person saw the hacker's August 11, 2023 post in the Hydra forum and sought to alert 23andMe users on an unofficial 23andMe user forum on Reddit that same day.[8]

6. For nearly two months, Defendant did nothing in response to the August 11, 2023 Hydra and Reddit posts, leaving Plaintiff and Proposed Class Members uninformed about the Data Breach.

7. In early October 2023, 23andMe user data misappropriated in the Data Breach appeared for sale on another hacking forum called BreachForums, including data that was claimed to come from "one million 23andMe users of Jewish Ashkenazi descent and 100,000 23andMe Chinese users."[9]

---

[4] FY 2022 10-K at 92.

[5] Lorenzo Franceschi-Bicchierai, *et al.*, *Hackers advertised 23andMe stolen data two months ago*, TechCrunch (Oct. 10. 2023), https://techcrunch.com/2023/10/10/hackers-advertised-23andme-stolen-data-two-months-ago/.

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *Id.*

8. Then, on October 6, 2023, 23andMe announced, via a blog post on its website (the "October 6 Blog Post"), that the Company had "recently learned that certain 23andMe customer profile information . . . was compiled from individual 23andMe.com accounts without the account users' authorization" as a result of "threat actors" being able to "access certain accounts."[10] The October 6 Blog Post attempted to blame 23andMe users, expressing Defendant's "belie[f]" that the Data Breach was the result of "threat actors [who] were able to access certain accounts in instances where users recycled login credentials—that is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked."[11]

9. Defendant's October 6 Blog Post did not provide any details about how many people were affected by the Data Breach and failed to mention that, as a result of the Data Breach, hackers had been selling a massive volume of 23andMe user data on the dark web for nearly two months.

10. Defendant updated its October 6 Blog Post on October 9, 2023 to report, among other things, that the Company had only recently engaged a third-party forensic expert and was "working with federal law enforcement."[12] Then, on October 20, 2023, 23andMe announced that it had temporarily disabled certain features on the DNA relatives tool. The October 6 Blog Post and the two updates thereto failed to provide basic details concerning the Data Breach, including, but not limited to, whether the breach was a system-wide breach, how many people were affected by the Data Breach, and whether certain populations, ethnic groups, or other identifiable categories of individuals were targeted in the cyberattack.

11. On December 5, 2023, Defendant again updated the Blog Post, revealing for the first time that the "threat actor" accessed "information included in a significant number of DNA Relatives profiles (approximately 5.5 million) and Family Tree feature profiles (approximately 1.4 million)."[13]

---

[10] 23andMe Blog, *supra,* note 1.

[11] *Id.*

[12] *Id.*

[13] *Id.*

12. 23andMe knowingly collected individuals' Private Information—notably including the most sensitive of all information conceivable, an individual's unique genetic information—in confidence. As a result, 23andMe had a duty to secure, maintain, protect, and safeguard that Private Information against unauthorized access and disclosure through reasonable and adequate security measures.

13. PHI is considered "the most confidential and valuable type of PII . . . irrevocable once breached."[14] There can be no more confidential and valuable form of PHI than an individual's unique and immutable genetic information.

14. 23andMe was aware of methods that would provide additional, heightened security that would safeguard its customers' highly sensitive data from unauthorized access and disclosure, including but not limited to requiring users to change their passwords frequently, requiring the use of "strong" passwords, and mandating the use of multi-factor authentication ("MFA") that would require its customers to enter more information than just a single password to access their accounts. Indeed, 23andMe acknowledges that while MFA "provides an extra layer of security and can prevent bad actors from accessing an account through recycled passwords," it concedes that it only "offered and encouraged" use of MFA starting in 2019.[15]

15. As a result of the Data Breach, Plaintiff and Proposed Class Members suffered ascertainable losses, including, but not limited to the value of their time spent to remedy or mitigate the effects of the Data Breach, out-of-pocket expenses from responding to the breach, and the loss of potential value of their private and confidential Private Information.

---

[14] Junyuan Ke, et al., *My Data or My Health? Heterogenous Patient Responses to Healthcare Data Breach*, SSRN (Feb. 10, 2022), http://dx.doi.org/10.2139/ssrn.4029103. Under the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. §§ 1320d, *et seq*., PHI is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered PHI under HIPAA, as are genetic data, national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *See Summary of the HIPAA Privacy Rule*, U.S. Dep't of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Dec. 7, 2023).

[15] 23andMe Blog, *supra* note 1.

16. Plaintiff and Proposed Class Members entrusted their Private Information to 23andMe, its officials, and agents. Plaintiff's and Proposed Class Members' Private Information was subsequently compromised, unlawfully accessed, and stolen due to the Data Breach.

17. Plaintiff brings this class action lawsuit on behalf of herself and all others similarly situated to address 23andMe's inadequate safeguarding of Plaintiff's and Proposed Class Members' Private Information, its failure to provide adequate notice to Plaintiff and other Proposed Class Members of the unauthorized access to their Private Information by a cyber attacker, and its failure to provide adequate notice of precisely what information was accessed and stolen.

18. 23andMe breached its duties to Plaintiff and Proposed Class Members by maintaining Plaintiff's and the Proposed Class Members' Private Information in a negligent and reckless manner.

19. Upon information and belief, the means of the Data Breach and potential risk for improper disclosure of Plaintiff's and Proposed Class Members' Private Information were known and foreseeable to 23andMe. Thus, 23andMe was on notice that failing to take steps necessary to secure Plaintiff's and Proposed Class Members' Private Information from those risks left the Private Information in a dangerous and vulnerable condition.

20. 23andMe and its employees failed to properly monitor the computer network and systems housing the Private Information. 23andMe claims that it "is committed to providing you with a safe and secure place where you can learn about your DNA knowing your privacy is protected" and that it "take[s] security seriously."[16] Moreover, the Company claims that:

> [W]e exceed industry data protection standards and have achieved three different ISO certifications to demonstrate the strength of our security program. We actively and routinely monitor and audit our systems to ensure that your data is protected. When we receive information through those processes or from other sources claiming customer data has been accessed by unauthorized individuals, we immediately investigate to validate whether this information is accurate.[17]

[16] 23andMe Blog, *supra* note 1.

[17] *Id.*

21. However, 23andMe failed to detect and stop the Data Breach. Moreover, 23andMe continues not to require heightened security practices, including but not limited to mandating the use of MFA and strong passwords.[18] Had 23andMe properly monitored its property and employed appropriate security measures commensurate with the sensitivity of the Private Information, it would have discovered the intrusion sooner or been able to prevent it altogether.

22. Exacerbating an already devastating privacy intrusion, Plaintiff's and Proposed Class Members' identities are now at a heightened risk of exposure because of 23andMe's negligent conduct because the Private Information that 23andMe collected and stored is now in the hands of data thieves or other malicious actors who may use the unlawfully obtained Private Information to the detriment of Plaintiff and Proposed Class Members.

23. Armed with the Private Information accessed in the Data Breach, data thieves can now use that data to commit a variety of crimes, including using Proposed Class Members' genetic, health, and ethnic information to target other phishing and hacking intrusions based upon their individual health needs or ethnic backgrounds. Moreover, data thieves or malicious actors who may have purchased or otherwise obtained Private Information from those who stole it may use that data to target Plaintiff and Proposed Class Members with violence or threats of harm based on animus toward members of particular ethnic groups. Indeed, the fact that initial leaks of Private Information stolen in the Data Breach and "advertised [for sale] on BreachForums allegedly contain one million 23andMe users of Jewish Ashkenazi descent and 100,000 23andMe Chinese users"[19] has prompted at least one State Attorney General to observe that "the increased frequency of antisemitic and anti-Asian rhetoric and violence in recent years means that this may be a particularly dangerous time for such targeted information to be released to the public."[20]

[18] *Id.* (including, as mere "Recommendations," that customers use strong passwords and enable MFA).

[19] Lorenzo Franceschi-Bicchierai et al., Hackers advertised 23andMe stolen data two months ago, *supra* note 5.

[20] William Tong, Att'y Gen. of Connecticut, Letter to Jacquie Cooke, General Counsel and Privacy Officer for 23andMe re: Data Breach (Oct. 30, 2023), https://portal.ct.gov/-/media/AG/Press_Releases/2023/10-30-2023-William-Tong--23andMe-Inc-Inquiry-Letter-final-002.pdf.

24. As a direct result of the Data Breach, Plaintiff and Proposed Class Members have suffered injury, and will continue to be exposed to a heightened and imminent risk of fraud and identity theft, potentially for the rest of their lives. Plaintiff and Proposed Class Members must now and in the future closely monitor their medical, healthcare, insurance, and financial accounts to guard against identity theft and potential healthcare frauds.

25. Plaintiff and Proposed Class Members may also incur out-of-pocket costs for purchasing protective measures to deter and detect identity theft and/or healthcare related fraud, as well as protective measures to mitigate against the misuse of their genetic information and related PHI.

26. As a direct and proximate result of the Data Breach and subsequent exposure of their Private Information, Plaintiff and Proposed Class Members have suffered, and will continue to suffer, damages and economic losses in the form of lost time needed to take appropriate measures to avoid the misuse of their Private Information including genetic information and PHI, potential unauthorized and fraudulent charges, and dealing with spam phone calls, letters, text messages, and emails received as a result of the Data Breach and the unauthorized disclosure and misuse of their Private Information.

27. Plaintiff and Proposed Class Members have suffered, and will continue to suffer, an invasion of their property interest in their own Private Information, such that they will be entitled to damages from 23andMe for unauthorized access to, theft of, and misuse of their Private Information.

28. These harms are ongoing, and Plaintiff and Proposed Class Members will suffer from future damages associated with the unauthorized use and misuse of their Private Information, as data thieves and malicious actors who purchase the stolen Private Information will continue to use the information to the detriment of Plaintiff and Proposed Class Members for several years, if not longer.

29. Plaintiff seeks to remedy these harms on behalf of all similarly situated individuals whose Private Information was accessed, compromised, and/or stolen during the Data Breach.

30. Accordingly, Plaintiff brings this action, on behalf of herself and all others similarly situated, against 23andMe seeking redress for its unlawful conduct asserting claims for (1) negligence, (2) negligence *per se*, (3) breach of implied contract, and (4) unjust enrichment.

PARTIES

A. Plaintiff

31. Plaintiff Julie MacMillan is an individual citizen and resident of Florida who is a victim of the Data Breach.

32. As a direct result of the Data Breach, Plaintiff has suffered injury and damages, including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of this highly sensitive Private Information; deprivation of the value of her Private Information; and overpayment for services that did not include adequate data security.

B. Defendant

33. Defendant 23andMe is a business incorporated under the laws of the state of Delaware with its principal place of business in California at 223 North Mathilda Avenue, Sunnyvale, California 94086. 23andMe is a genetic testing company that designs its products in California, and its marketing efforts emanate from California.

JURISDICTION AND VENUE

34. This Court has jurisdiction over this action and the parties.

35. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than one hundred members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

36. This Court has personal jurisdiction over the Defendant because Defendant is headquartered in California and within this District, has its principal place of business in Santa Clara County, California and within this District, and it regularly conducts business in California and within this District.

37. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant's principal place of business is located in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District.

FACTUAL ALLEGATIONS

A. Defendant 23andMe's Business

38. 23andMe purports to be a leading consumer genetics and research company, founded in 2006, that describes its mission as helping people access, understand, and benefit from the human genome. According to the "Corporate Profile" on its website, 23andMe "want[s] to disrupt the healthcare experience by building a personalized health and wellness experience that caters uniquely to the individual by harnessing the power of their DNA" and touts itself as having "pioneered direct access to genetic information" as "the only company with multiple FDA clearances for genetic health reports."[21]

39. As stated in its last annual report filed with the U.S. Securities and Exchange Commission, as of March 31, 2023, 23andMe has approximately 14.1 million customers who have supplied their Private Information to the Company.[22]

40. This Private Information includes genetic information provided by individuals since 2006 in connection with the Company's "Personal Genome Service" business, which purports to provide consumers "with a broad suite of genetic reports, including information on customers' genetic ancestral origins, personal genetic health risks, and chances of passing on certain rare carrier conditions to their children, as well as reports on how genetics can impact responses to medication."[23]

B. The Collection of Plaintiff's and Proposed Class Members' Private Information is Central to 23andMe's Business

41. In order for 23andMe to offer its services to customers including Plaintiff and the Proposed Class Members, Plaintiff and Proposed Class Members were required to transfer

[21] 23andMe Investor Relations, *supra* note 2.

[22] FY 2022 10-K at 69.

[23] *Id.* at 92.

possession of their Private Information—specifically including personal genetic material—to 23andMe. 23andMe thereby acquires and electronically stores Private Information provided to it by its customers. Accordingly, 23andMe was required to ensure that Plaintiff's and Proposed Class Members' Private Information was not disclosed or disseminated to unauthorized third parties.

42. Through the possession and use of Plaintiff's and Class Members' Private Information, 23andMe assumed duties owed to Plaintiff and Proposed Class Members regarding the care and safeguarding of their Private Information. Therefore, 23andMe knew or should have known that it was responsible for safeguarding Plaintiff's and Proposed Class Members' Private Information from unauthorized access and misuse.

43. 23andMe has publicly touted its data security and cybersecurity abilities, including stating that the Company "is committed to providing you with a safe and secure place where you can learn about your DNA knowing your privacy is protected" and that it "take[s] security seriously."[24]

44. 23andMe assures customers that "[y]our privacy comes first."[25] "When you explore your DNA with 23andMe, you entrust us with important personal information. That's why, since day one, protecting your privacy has been our number one priority. We're committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected."[26]

45. 23andMe's customers are also told that their genetic data will not be shared with third parties "without your explicit consent" and that "[y]our data is fiercely protected by security practices that are regularly reviewed an updated" and the Company is "doing everything in our power to keep your personal data safe."[27]

46. Plaintiff and Proposed Class Members relied on 23andMe to keep their Private Information secure and safeguarded against unauthorized access and disclosure to unauthorized

[24] 23andMe Blog, *supra* note 1.

[25] 23andMe Privacy, Privacy and Data Protection, 23andMe, Inc., https://www.23andme.com/privacy/ (last accessed Dec. 7, 2023).

[26] *Id.*

[27] *Id.*

persons. 23andMe owed a duty to Plaintiff and Proposed Class Members to secure their Private Information and ultimately breached that duty.

C. The Data Breach

47. According to news reports, on or about August 11, 2023, "a hacker on a known cybercrime forum called Hydra advertised a set of 23andMe user data."[28] The hacker claimed "to have 300 terabytes of stolen 23andMe user data" that it would sell for $50 million, and offered to sell "a subset of data" for between $1,000 and $10,000.[29] The hacker also purportedly indicated that they had contacted 23andMe, "'but instead of taking the matter seriously, [the Company] asked irrelevant questions.'"[30] At least one person saw the hacker's August 11, 2023 post in the Hydra forum and sought to alert 23andMe users on an unofficial 23andMe user forum on Reddit that same day.[31]

48. In early October 2023, 23andMe user data misappropriated in the Data Breach appeared for sale on another hacking forum called BreachForums, including data that was claimed to come from "one million 23andMe users of Jewish Ashkenazi descent and 100,000 23andMe Chinese users."[32]

49. Defendant did not acknowledge or address the Data Breach until October 6, 2023, when it posted the October 6 Blog Post on its website. The October 6 Blog Post states:

> We recently learned that certain 23andMe customer profile information that they opted into sharing through our DNA Relatives feature, was compiled from individual 23andMe.com accounts without the account users' authorization.
>
> After learning of suspicious activity, we immediately began an investigation. While we are continuing to investigate this matter, we believe threat actors were able to access certain accounts in instances where users recycled login credentials – that is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked.

[28] Lorenzo Franceschi-Bicchierai et al., *Hackers advertised 23andMe stolen data two months ago*, *supra* note 5.

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.*

> We believe that the threat actor may have then, in violation of our Terms of Service, accessed 23andMe.com accounts without authorization and obtained information from certain accounts, including information about users' DNA Relatives profiles, to the extent a user opted into that service.
>
> Committed to Safety and Security
>
> 23andMe is committed to providing you with a safe and secure place where you can learn about your DNA knowing your privacy is protected. We are continuing to investigate to confirm these preliminary results. We do not have any indication at this time that there has been a data security incident within our systems, or that 23andMe was the source of the account credentials used in these attacks.
>
> At 23andMe, we take security seriously. We exceed industry data protection standards and have achieved three different ISO certifications to demonstrate the strength of our security program. We actively and routinely monitor and audit our systems to ensure that your data is protected. When we receive information through those processes or from other sources claiming customer data has been accessed by unauthorized individuals, we immediately investigate to validate whether this information is accurate. Since 2019 we've offered and encouraged users to use multi-factor authentication (MFA), which provides an extra layer of security and can prevent bad actors from accessing an account through recycled passwords.
>
> Recommendations
>
> We encourage our customers to take as much action to keep their account and password secure. Out of caution, we recommend taking the following steps:
>
> - Confirm you have a strong password, one that is not easy to guess and that is unique to your 23andMe account. If you are not sure whether you have a strong password for your account, reset it by following the steps outlined here.
> - Please be sure to enable multi-factor authentication (MFA) on your 23andMe account. You can enable MFA by following the steps outlined here.
> - Review our Privacy and Security Checkup page with additional information on how to keep your account secure.[33]

50. While the October 6 Blog Post did not expressly indicate the scope of the Data Breach in terms of the numbers of users affected or recite the categories of Private Information that were exposed, compromised, and stolen by unauthorized third parties, the categories of information

[33] 23andMe Blog, *supra* note 1.

in the "DNA Relatives feature" referenced by Defendant include: (1) names; (2) sex (3) dates of birth; (4) genetic information that includes (but is not limited to) maternal and paternal haplogroup results and neanderthal ancestry results; (5) predicted relationships with genetic matches; (6) ancestry reports; (7) ancestors' birth locations and family names; (8) Family tree information; (9) profile pictures; and (10) geographic location.[34]

51. 23andMe's notice to Plaintiff and Proposed Class Members was untimely and woefully deficient, failing to provide basic details concerning the Data Breach, including but not limited to how unauthorized third parties were able to access Private Information, what Private Information was in fact compromised, and how many people were affected by the Data Breach.

52. Given the criminal nature of the cybersecurity attack and Data Breach, Plaintiff's and Proposed Class Members' Private Information is now for sale to criminals on the dark web—as was first shown by the August 11, 2023 posts on the Hydra message board—meaning unauthorized parties have for months accessed and viewed Plaintiff's and Proposed Class Members' unencrypted, unredacted Private Information, including their highly sensitive genetic data and more.

D. Plaintiff's Experience

53. Plaintiff discovered on or about December 5, 2023 that her Private Information, including her genetic material, was very likely included in the data accessed through the Data Breach when the news media reported that the Data Breach impacted a total of 6.9 million victims as a result of the threat actor accessing the information of users "who opted-in to 23andMe's DNA Relatives feature, which allows customers to automatically share some of their data with others."[35]

54. Plaintiff purchased a 23andMe kit between 2016 and 2017 and provided a sample of her genetic material to 23andMe for testing. Ms. MacMillan was required to provide her Private Information, including her genetic material, to 23andMe in order to become a customer of 23andMe.

[34] 23andMe Customer Care, *DNA Relatives Privacy & Display Settings*, 23andMe, Inc., https://customercare.23andme.com/hc/en-us/articles/212170838 (last accessed Dec. 7, 2023).

[35] Lorenzo Franceschi-Bicchierai, *23andMe confirms hackers stole ancestry data on 6.9 million users*, TechCrunch (Dec. 4, 2023), https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/.

At the time of the Data Breach, Ms. MacMillan's Private Information was maintained on 23andMe's computer systems.

55. At all relevant times, Plaintiff has opted-in to the DNA Relatives feature.

56. The Private Information that was accessed in the Data Breach was the kind of sensitive information that can be used to commit fraud and identity theft. It is reasonable and foreseeable that Ms. MacMillan would take, and will continue to take, necessary measures to protect her Private Information.

57. Ms. MacMillan has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in 23andMe's possession, is protected and safeguarded from further and future breaches.

58. Ms. MacMillan suffered actual injury in the form of damages to and loss of potential value of her Private Information—a form of intangible property that Ms. MacMillan entrusted to 23andMe for the purpose of receiving healthcare services, which was compromised in, and as a result, of the Data Breach.

59. As a result of the Data Breach, Ms. MacMillan has suffered emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, and using his Private Information.

60. As a result of the Data Breach, Ms. MacMillan will continue to be at heightened risk for harassment, financial fraud, medical fraud, and identity theft, and the attendant damages, for years to come.

E. <u>The Healthcare Sector Is Particularly Susceptible to Cyberattacks</u>

61. As a company that holds itself out as seeking to "disrupt the healthcare experience by building a personalized health and wellness experience that caters uniquely to the individual by harnessing the power of their DNA," 23andMe was or should have been on notice that the Federal Bureau of Investigation ("FBI") has been concerned about data security in the healthcare and genetic information sector. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "'[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps

for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII).'"[36]

62. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[37]

63. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[38] In 2022, 1,802 data compromises that impacted over 422 million victims were reported, marking a forty-two percent increase in the number of victims impacted since 2021.[39] That upward trend continues.

64. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[40] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential, genetic data by virtue of its immutable nature, more so.

65. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and the victims were often

---

[36] Jim Finkle, *FBI warns healthcare firms that they are targeted by hackers*, Reuters (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[37] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (emphasis omitted).

[38] Press Release, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, CyberScout, Cision PR Newswire (Jan. 19, 2017), https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html.

[39] Identity Theft Resource Center, *2022 Data Breach Report*, Identity Theft Res. Ctr. (Jan. 2023), https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf.

[40] *Identity Theft Resource Center, 2018 End-of-Year Data Breach Report*, Identity Theft Res. Ctr. (2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINALWEB-V2-2.pdf.

forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[41] Almost 50% of the victims lost their healthcare coverage as a result of the incident, while nearly thirty percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and a detrimental impact on the economy as a whole.[42]

66. Healthcare related data breaches also come at a cost to the breached entities. According to IBM's 2023 Cost of a Data Breach Report, the healthcare sector reported the highest data breach costs for the thirteenth year in a row in 2023—increasing 8.2% from $10.10 million in 2022 to $10.93 million in 2023.[43] This cost should only further create incentive for service providers such as 23andMe both to invest in and implement reasonable and adequate security measures to avoid financial repercussions in the event of a breach.

67. Healthcare related data breaches have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, eighty-two percent of participating hospital information security leaders reported having a significant security incident in the last twelve months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[44]

> Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information (PII) for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.[45]

68. As an entity whose entire business model depends on the handling, storing, and safeguarding of PII and PHI—notably including genetic information, which is perhaps the most

---

[41] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[42] *Id.*

[43] IBM, *Cost of a Data Breach Report 2023*, at 13, https://www.ibm.com/downloads/cas/E3G5JMBP.

[44] HIMSS, *2019 HIMSS Cybersecurity Survey*, HIMSS (2019) at 4, https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf.

[45] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Chief Healthcare Exec. (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

unique, critical, and sensitive type of Private Information, 23andMe knew, or reasonably should have known, the importance of safeguarding the Private Information entrusted to it, and of the foreseeable consequences if its data security systems were breached. 23andMe failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

F. The Value of Private Information and the Effects of Unauthorized Disclosure

69. At all relevant times, 23andMe knew that the Private Information it collects from Plaintiff and Proposed Class Members is highly sensitive, immutable, and of significant value to those who would use it for wrongful purposes.

70. Private Information is a valuable commodity to cyber attackers. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[46] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground websites, commonly referred to as the dark web.

71. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363.47. In this particular instance, hackers have specifically offered for sale 300TB of 23andMe data for $50 million, with certain subsets of data available for between $1,000 and $10,000.[48] Moreover, 23andMe recently entered into an agreement with the pharmaceutical giant GSK Plc to sell one year of non-exclusive access to 23andMe customer data for $20 million.[49]

72. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's genetic makeup, ancestry or lineage, medical

[46] FTC Consumer Advice, *What to Know About Identity Theft*, Fed. Trade Comm'n, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed Dec. 7, 2023).

[47] Center For Internet Security, *Data Breaches: In the Healthcare Sector*, Ctr. for Internet Sec., https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed Dec. 7, 2023).

[48] Lorenzo Franceschi-Bicchierai et al., *Hackers advertised 23andMe stolen data two months ago*, *supra* note 5.

[49] Press Release, 23andMe, *23andMe Announces Collaboration Extension with a New Data Licensing Agreement with GSK*, 23andMe, Inc. (Oct. 30, 2023), https://investors.23andme.com/node/8996/pdf.

conditions, or victim settlements. It can also be used to create fake insurance claims, purchase and resell medical equipment, or gain access to prescriptions for illegal use or resale.

73. Genetic identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "'Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery,'" reported Pam Dixon, executive director of World Privacy Forum. According to Dixon, "'Victims often experience financial repercussions, and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities.'"[50]

74. The ramifications of 23andMe's failures to keep Plaintiff's and Proposed Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years and here, potentially for the rest of the victims' lives given that one's genetic information is immutable by nature and utterly irreplaceable. Fraudulent activity might not show up for six to 12 months or even longer.

75. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

76. Many victims do not realize their identity has been compromised until years after it has happened.[51] This gives thieves ample time to seek multiple treatments under the victim's name and perpetuate elaborate, costly frauds. Most consumers find out they were a victim of medical identity theft only when they receive collection letters from creditors for expenses that were incurred in their names.[52]

[50] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KFF Health News (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft.

[51] IdentityForce, *Medical ID Theft Checklist*, (Jan. 12, 2023), https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[52] *Id.*

77. As a company whose entire business model is dependent on the collection and use of highly sensitive Private Information including genetic information, 23andMe knew, or reasonably should have known, the importance of safeguarding Plaintiff's and Proposed Class Members' Private Information and the foreseeable consequences if its data security systems were breached. Those consequences include the significant costs that would be imposed on Plaintiff and Proposed Class Members as a result of a breach. 23andMe failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

G. 23andMe Failed to Comply with FTC Guidelines

78. 23andMe was also prohibited by the Federal Trade Commission Act ("FTCA") from engaging in "unfair or deceptive acts or practices in or affecting commerce."[53] The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA.[54]

79. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[55]

80. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[56] The guidelines set forth that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[57]

[53] 15 U.S.C. § 45(a)(1).

[54] *See, e.g., In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020) (citing *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)).

[55] FTC, *Start With Security: A Guide for Business, Lessons Learned From FTC Cases*, Fed. Trade Comm'n (Jun. 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[56] FTC, *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[57] *Id.*

81. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

82. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Further orders resulting from these actions clarify the measures businesses must take to meet data security obligations.

83. 23andMe failed to properly implement basic data security practices. 23andMe's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Proposed Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

84. 23andMe was fully aware of its obligations to protect the Private Information of Plaintiff and Proposed Class Members because of its position as a service provider whose business centers on the collection, storage, and safeguarding of PII and PHI. 23andMe was also aware of the significant repercussions that would result from its failure to make good on those obligations.

H. Cyber Criminals Have and Will Continue to Use Plaintiff's and Proposed Class Members' PII and PHI for Nefarious Purposes

85. Plaintiff's and Proposed Class Members' highly sensitive Private Information is of great value to cybercriminals, who can use the data stolen in the Data Breach to exploit Plaintiff and the Proposed Class Members and profit off their misfortune and stolen information. The cybercriminals' motives for the Data Breach were purely nefarious and malicious in nature: their one goal was to access systems, including 23andMe's systems, in order to obtain valuable PII and PHI to sell on the dark web. Indeed, hackers likely have been selling 23andMe customers' Private Information on the dark web since approximately August 11, 2023.

86. Every year, identity theft causes tens of billions of dollars of losses to victims in the United States.[58] Those losses occur when identity thieves open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[59] Plaintiff and Proposed Class Members are at risk of suffering those same losses. Those criminal activities are likely to result in devastating financial and personal losses to Plaintiff and Proposed Class Members.

87. PII is such a valuable commodity to identity thieves that, once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.

88. Those risks are both certainly impending and substantial. As the FTC has reported, if cyber attackers get access to PII, they will use it.[60]

89. Cyber attackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[61]

90. If cyber criminals manage to access PII, health insurance information, and other personally sensitive data, as is the case with this Data Breach, there is no limit to the amount of fraud to which 23andMe may have exposed Plaintiff and Proposed Class Members.

---

[58] Insurance Information Institute, *Facts + Statistics: Identity Theft and Cybercrime*, Ins. Info. Inst. (2023), https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last accessed Nov. 6, 2023).

[59] Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, USA Today (Nov. 15, 2017), https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/

[60] Ari Lazarus, *How fast will identity thieves use stolen info?*, Military Consumer (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.

[61] U.S. Government Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, Gov't Accountability Off. (Jul. 5, 2007) at 29, https://www.gao.gov/assets/gao-07-737.pdf.

I. Plaintiff and Proposed Class Members Suffered Damages

91. The ramifications of 23andMe's failures to keep Plaintiff's and Proposed Class Members' Private Information secure are long, lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[62]

92. In addition to their obligations under state laws and regulations, 23andMe owed a common law duty to Plaintiff and Proposed Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties. That duty extends to 23andMe's obligations to conduct ongoing, robust due diligence into its routine security practices.

93. 23andMe further owed and breached its duties to Plaintiff and Proposed Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to act timely upon warnings and alerts, including those generated by its own security systems. Instead of implementing such processes and specifications, 23andMe allowed the Data Breach to go undetected for an unknown period of time before recognizing unusual activity.

94. As a direct result of 23andMe's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, cyber attackers were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse of Plaintiff's and Proposed Class Members' Private Information as detailed above, and Plaintiff and Proposed Class Members are now at a heightened risk of harassment, identity theft, and healthcare and insurance fraud.

95. The risks associated with identity theft are serious. Victims often may be required to spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities or be denied loans

[62] LexisNexis, *2014 LexisNexis True Cost of Fraud Study, Post-Recession Revenue Growth Hampered by Fraud as All Merchants Face Higher Costs*, LexisNexis (Aug. 2014) at 6, https://risk.lexisnexis.com/-/media/files/corporations%20and%20non%20profits/research/true-cost-fraud-2014%20pdf.pdf.

for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

96. The U.S. Department of Justice's ("DOJ") Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "[r]esolving the problems caused by identity theft [could] take more than a year for some victims."[63] The costs for dealing with the theft of genetic information may be much more because they could result in healthcare or other complicated frauds.

97. In this case, other risks beyond identity theft exist due to the disclosure of highly sensitive genetic information, such as the unauthorized access to and/or disclosure of individuals' ethnic heritage and/or revealing an individuals' potentially heightened risk for certain health problems. Publicly outing this sensitive information increases the risk of harassment, threats, or unwanted marketing from malicious actors aligning their malicious or unwanted outreach to information contained in one's private genetic profile. Unlike replacing a stolen credit card in the case of a financial fraud due to identity theft, genetic data by its nature is fixed, and as such, once a fraud using stolen genetic information is perpetrated, an affected individual has little to no recourse to undo the theft because genetic information is immutable.

98. Plaintiff and Proposed Class Members did not receive the full benefit of the bargain for received services. As a result, Plaintiff and Proposed Class Members were damaged in an amount at least equal to the difference in the value of the genetic information services they paid for and the services they received without the data security protection.

99. As a result of the Data Breach, Plaintiff's and Proposed Class Members' Private Information has lost potential value.

100. The Private Information belonging to Plaintiff and Proposed Class Members is private in nature and was left inadequately protected by 23andMe. 23andMe did not obtain Plaintiff's or Proposed Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

[63] Erika Harrell et al., *Victims of Identity Theft*, 2012, DOJ, Off. of Just. Programs Bureau of Just. Stats. (Dec. 2013) at 1, 11, https://www.bjs.gov/content/pub/pdf/vit12.pdf.

101. The Data Breach was a direct and proximate result of 23andMe's failure to (1) properly safeguard and protect Plaintiff's and Proposed Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law, (2) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Proposed Class Members' Private Information, and (3) protect against reasonably foreseeable threats to the security or integrity of such information. Among other things, 23andMe failed to employ measures that the Company acknowledges provide heightened security such as requiring customers to use MFA, frequently change passwords, and use strong passwords associated with their 23andMe accounts.

102. 23andMe had the resources necessary to prevent the Data Breach but neglected to adequately implement data security measures, despite its obligation to protect genetic data.

103. Had 23andMe remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into their systems and, ultimately, the theft of Plaintiff's and Proposed Class Members' Private Information.

104. As a direct and proximate result of 23andMe's wrongful actions and inactions, Plaintiff and Proposed Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

105. 23andMe's failures to adequately protect Plaintiff's and Proposed Class Members' Private Information has resulted in Plaintiff and Proposed Class Members having to undertake those tasks, which require extensive amounts of time and, for use of many credit and fraud protection services, payment of money. Rather than assist those affected by the Data Breach, 23andMe has put the burden on Plaintiff and Proposed Class Members to discover possible fraudulent activity and identity theft.

106. As a result of 23andMe's failures to prevent the Data Breach, Plaintiff and Proposed Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in their possession;

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Proposed Class Members; and

f. Anxiety and distress resulting from fear of misuse of their genetic information.

107. In addition to a remedy for the economic harm, Plaintiff and Proposed Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

J. 23andMe's Delay in Identifying and Reporting the Breach Caused Additional Harm

108. It is well-documented that:

> [T]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these

> organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[64]

Here, the same applies to 23andMe and the unauthorized access to Plaintiff's and Proposed Class Members' accounts.

109. Indeed, once a data breach has occurred,

> [O]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers . . . If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves.[65]

110. Although their Private Information was improperly exposed on or before August 11, 2023, Plaintiff and Proposed Class Members were not notified until October 6, 2023. 23andMe's delay deprived Plaintiff and Proposed Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

111. As a result of 23andMe's delay in detecting and notifying individuals of the Data Breach, the risk of fraud for Plaintiff and Proposed Class Members has been driven even higher, a warning state Attorneys General have alluded to when questioning 23andMe about its "unreasonable delay" in notifying affected consumers about the Data Breach.[66]

CLASS ALLEGATIONS

112. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

113. Plaintiffs bring this action on behalf of themselves and all members of the following National Class of similarly situated persons:

---

[64] Javelin Strategy & Research, *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire (Feb. 1, 2017), https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million.

[65] Allen St. John, *The Data Breach Next Door*, Consumer Reports (Jan. 31, 2019), https://www.consumerreports.org/data-theft/the-data-breach-next-door/.

[66] William Tong, Letter to Jacquie Cooke, General Counsel and Privacy Officer for 23andMe, *supra* note 20.

> All individuals in the United States whose Private Information was compromised or disclosed to unauthorized persons in the Data Breach.

114. Excluded from the Class is 23andMe, Inc., and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

115. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

116. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in an individual actions alleging the same claims.

117. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. To date, Defendant has identified at least 6.9 million users whose Private Information may have been improperly accessed and compromised in the Data Breach.

118. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Proposed Class Members. These include:

a. Whether and when Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining Proposed Class Members' Private Information;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Proposed Class Members' Private Information;

e. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Proposed Class Members' Private Information;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Proposed Class Members' Private Information secure and prevent loss or misuse of that Private Information;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff's and Proposed Class Members' damages;

i. Whether Defendant violated the law by failing to promptly notify Proposed Class Members that their Private Information had been compromised;

j. Whether Plaintiff and the other Proposed Class Members will be entitled to actual damages, extended credit monitoring, and other monetary relief; and

k. Whether Defendant violated common law and statutory claims alleged herein.

119. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Proposed Class Members, because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

120. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect the Class uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

121. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of Proposed Class Members. She has no conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class, and the infringement of the rights and the damages she has

suffered are typical of other Proposed Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

122. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class action litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Proposed Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Proposed Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Proposed Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

123. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because (1) Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of the Class with superior financial and legal resources, (2) the costs of individual suits could unreasonably consume the amounts that would be recovered, (3) proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged, and (4) individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

124. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Proposed Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

125. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

126. Unless a Class-wide injunction is issued, Plaintiff and Proposed Class Members remain at risk that Defendant will continue to fail to properly secure the Private Information of Plaintiff and Proposed Class Members resulting in another data breach, continue to refuse to provide proper notification to Proposed Class Members regarding the Data Breach, and continue to act unlawfully as set forth in this Class Action Complaint.

127. Defendant acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

128. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Proposed Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable and adequate security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Proposed Class Members are entitled to additional credit monitoring or other injunctive relief, and will be entitled to actual damages, and/or punitive damages as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

129. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

130. Plaintiff and Proposed Class Members were required to submit their Private Information to Defendant in order to receive services from Defendant.

131. Defendant knew, or should have known, of the risks inherent in collecting and storing the Private Information of Plaintiff and Proposed Class Members.

132. As described above, Defendant owed duties of care to Plaintiff and Proposed Class Members whose Private Information had been entrusted with Defendant.

133. Defendant breached its duties to Plaintiff and Proposed Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Proposed Class Members' Private Information.

134. Defendant acted with wanton disregard for the security of Plaintiff's and Proposed Class Members' Private Information. Defendant knew or reasonably should have known that it had inadequate data security practices to safeguard such information, and Defendant knew or reasonably should have known that data thieves were attempting to access databases containing PII and PHI, such as those of Defendant.

135. A "special relationship" exists between Defendant and Plaintiff and Proposed Class Members. Defendant entered into a "special relationship" with Plaintiff and Proposed Class Members because Defendant collected the Private Information of Plaintiff and the Proposed Class Members—information that Plaintiff and the Proposed Class Members were required to provide in order to receive services from Defendant.

136. But for Defendant's wrongful and negligent breaches of the duties owed to Plaintiff and the Proposed Class Members, Plaintiff and the Proposed Class Members would not have been injured.

137. The injury and harm suffered by Plaintiff and Proposed Class Members was the reasonably foreseeable result of Defendant's breaches of its duties. Defendant knew or reasonably should have known it was failing to meet its duties, and that Defendant's breaches of such duties would cause Plaintiff and Proposed Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

138. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Proposed Class Members have suffered injury and are entitled to injunctive relief. Plaintiffs and Proposed Class Members have suffered economic damages as well, in an amount to be proven at trial.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

139. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

140. Pursuant to the FTCA (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate data security practices to safeguard Plaintiff's and Proposed Class Members' Private Information.

141. Defendant breached its duties to Plaintiff and Proposed Class Members under the FTCA (15 U.S.C. § 45) by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiff's and Proposed Class Members' Private Information.

142. Defendant's failures to comply with applicable laws and regulations constitutes negligence *per se*.

143. But for Defendant's wrongful and negligent breaches of their duties owed to Plaintiff and Proposed Class Members, Plaintiff and Proposed Class Members would not have been injured.

144. The injury and harm suffered by Plaintiff and Proposed Class Members was the reasonably foreseeable result of Defendant's breaches of its duties. Defendant knew or reasonably should have known that it was failing to meet their duties, and that Defendant's breaches would

cause Plaintiff and Proposed Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

145. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Proposed Class Members have suffered and are entitled to injunctive relief. Plaintiffs and Proposed Class Members have suffered economic damages as well, in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

146. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

147. Plaintiff and Proposed Class Members entered into an implied contract with Defendant when they sought or obtained services from Defendant, in exchange for which they were required to provide their Private Information. The Private Information provided by Plaintiff and Proposed Class Members to Defendant was governed by and subject to Defendant's representations about privacy and security and its privacy duties and policies.

148. Defendant agreed to safeguard and protect the Private Information of Plaintiff and Proposed Class Members and to timely and accurately notify Plaintiff and Proposed Class Members in the event that their Private Information was breached or otherwise compromised.

149. Plaintiff and Proposed Class Members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Proposed Class Members believed that Defendant would use part of the monies paid to Defendant under the implied contracts to fund adequate and reasonable data security practices.

150. Plaintiff and Proposed Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract or implied terms between Plaintiff and Proposed Class Members and Defendant. The safeguarding of the Private Information of Plaintiff and Proposed Class Members and prompt and sufficient notification of a breach involving Private Information was critical to realize the intent of the parties.

151. Plaintiff and Proposed Class Members fully performed their obligations under the implied contracts with Defendant.

152. Defendant breached its implied contracts with Plaintiff and Proposed Class Members to protect Plaintiff's and Proposed Class Members' Private Information when it (1) failed to have data security practices in place to protect that information; (2) disclosed that information to unauthorized third parties; and (3) failed to provide timely and accurate notice that their Private Information was compromised as a result of the Data Breach.

153. As a direct and proximate result of Defendant's breaches of implied contract, Plaintiff and Proposed Class Members are entitled to injunctive relief. Plaintiff and Proposed Class Members have suffered economic damages as well, in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

154. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

155. This Count is pleaded in the alternative to the breach of implied contract claim above (Count III).

156. Plaintiff and Proposed Class Members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information—Private Information that has inherent value. In exchange, Plaintiff and Proposed Class Members should have been entitled to Defendant's adequate storage and safeguarding of their Private Information.

157. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Proposed Class Members.

158. Defendant benefitted from Plaintiff's and Proposed Class Members' retained Private Information and used their Private Information for business purposes.

159. Defendant failed to store and safeguard Plaintiff's and Proposed Class Members' Private Information. Had Plaintiff and Proposed Class Members known that Defendant was unable to adequately store and safeguard their Private Information, they would not have agreed to provide such Private Information to Defendant.

160. As a result of Defendant's failures, Plaintiff and Proposed Class Members suffered actual damages in an amount equal to the difference in value between the services with the adequate data privacy and security practices that Plaintiff and Proposed Class Members bargained for and the services without adequate data privacy and security practices that they received.

161. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Proposed Class Members because Defendant failed to implement—or adequately implement—the data privacy and security practices that Plaintiff and Proposed Class Members paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

162. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Proposed Class Members all unlawful or inequitable proceeds received by Defendant.

163. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendant traceable to Plaintiff and Proposed Class Members.

PRAYER FOR RELIEF

Plaintiff, individually, and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against 23andMe as follows:

A. certifying the Class as requested herein, designating Plaintiff as a Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent 23andMe from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: January 30, 2024

KAPLAN FOX & KILSHEIMER LLP

By: /s/ *Laurence D. King*
Laurence D. King

Laurence D. King (SBN 206423)
Matthew B. George (SBN 239322)
Blair E. Reed (SBN 316791)
Clarissa R. Olivares (SBN 343455)
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Telephone: (415) 772-4700
Facsimile: (415) 772-4707
Email: *lking@kaplanfox.com*
mgeorge@kaplanfox.com
breed@kaplanfox.com
colivares@kaplanfox.com

BONI, ZACK & SNYDER LLC
Michael J. Boni
Joshua D. Snyder (*pro hac vice application forthcoming*)
Benjamin J. Eichel (*pro hac vice application forthcoming*)
15 St. Asaphs Road
Bala Cynwyd, PA 19004
Tel: 610-822-0200
Fax: 610-822-0206
Email: *mboni@bonizack.com*
jsnyder@bonizack.com
beichel@bonizack.com

SALTZ, MONGELUZZI & BENDESKY, PC
Simon B. Paris (*pro hac vice application forthcoming*)
Patrick Howard (*pro hac vice application forthcoming*)
1650 Market Street, 52nd Floor
Philadelphia, PA 19103
Tel: 215-575-3986
Fax: 215-754-4443
Email: *sparis@smbb.com*
phoward@smbb.com

Attorneys for Plaintiff and the Proposed Class